1. Contact Information

Department of State Privacy Coordinator
Sheryl Walter Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: March 2012

(b) Name of system: International Vetting and Security Tracking

(c) System acronym: INVEST

(d) IT Asset Baseline (ITAB) number: 4387

(e) System description (Briefly describe scope, purpose, and major functions):

The Leahy Vetting system enables the State Department to vet foreign security force candidates and units for credible evidence of violations of human rights prior to receiving training or security assistance programs from the U.S. Government. All individuals vetted are foreign nationals.

(f) Reason for performing PIA:

X New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable):

(h) Date of previous PIA (if applicable):

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

X does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

Elements collected are an individual's name, alias (if any), gender, date of birth, citizenship, rank, branch and unit of foreign security force, and whether any evidence of human rights violations was found. These individuals are primarily foreign nationals but, in rare cases, can also be American citizens or those with dual citizenship. Two databases maintained by DRL are the source of this information. The first is a work flow and work trail database, and it tracks the records and information on each candidate. When an INVEST user finds any information on a candidate, he or she notes this in this first database. It serves as a complete source for all information on a candidate, from

the vetting to the auditing. Also, this database will store any derogatory non-human rights information discovered during open source vetting.

The second database, the INVEST Document Library, contains supporting documentation for claims made in the first database. For example, if the first database states that a candidate was found to have tortured a citizen in Guatemala, a newspaper article discussing this incident would be included in the second database. All information used can be considered public.

b. How is the information collected?

Relevant information found on the Internet, in office records, or through internal searches is captured and attached by users of INVEST to the electronic file of the individual or unit being vetted contained in the INVEST Document Library referred to in section 3(a).

c. Why is the information collected and maintained?

Due to legislation related to the Departments of State and Defense foreign assistance to foreign security forces and due to policy concerns, individual and unit vetting needs to take place. The information is collected and maintained so that an individual or military unit that has been identified as having derogatory human rights records does not receive government training or assistance.

d. How will the information be checked for accuracy?

The regional bureau, post, DRL, and other bureaus, including INR as appropriate, will jointly assess the veracity of the information.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The authority supporting the collection of this information follows:

- The State Leahy Law, Section 620M of the Foreign Assistance Act, as amended, states, "No assistance shall be furnished under this Act or the Arms Export Control Act to any unit of the security forces of a foreign country if the Secretary of State has credible information that such a unit has committed gross violations of human rights." The State Department implements this provision by conducting Leahy vetting to determine whether the Department has such evidence prior to providing assistance or training.

There is a second Leahy law found as recurring language in the annual Defense Appropriations Act, which affects DOD-funded training. This provision states: "None of the funds made available by this act may be used to support any training program involving a unit of the security forces of a foreign country if the Secretary of Defense had received credible information for the Department of State that the unit has committed a gross violation of human rights, unless all necessary corrective steps have been taken." Upon request by DOD, the State Department also performs Leahy vetting for DOD-funded programs under this provision.

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The amount and type of PII collected on foreign security force candidates poses the minimal threat possible to the candidate while still achieving the goal of vetting them for

human rights violations. Due to the inclusion of data on possible human rights violations by individuals, the sensitivity of the information contained in INVEST is elevated. However, the information on human rights violations is critical to the purpose of INVEST and is the only sensitive information collected.

4. Uses of the Information

a. Describe all uses of the information.

The information is used to validate an individual or individuals' identities and to prevent security force training or assistance from being provided should credible evidence be found indicating the party or parties committed gross human rights violations.

b. What types of methods are used to analyze the data? What new information may be produced?

The methods used to analyze data depend upon the source and nature of the information. The regional bureau, post, DRL, and other bureaus, as appropriate, will jointly assess the veracity and significance of the information. INVEST does not utilize data mining in analyzing data.

No new information is produced in INVEST. Instead, it serves as a repository for information gathered outside the system.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Such information would be used as reference material for determining if the person or unit being vetted should receive training or assistance. Publicly available information, as well as information from other Federal agency databases, is researched and may be attached to the electronic file of the individual being investigated for the determination of his or her eligibility for training. Attaching classified information to the electronic file is prohibited.

d. Are contractors involved in the uses of the PII?

Congressionally-earmarked funds are used to hire vetters in regional bureaus and DRL. Some vetting is conducted by contractors hired specifically for that purpose, while some vetting is done by Civil Service and Foreign Service nationals.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

- Users must have a State Department network logon account
- The use of information collected in INVEST is for a specific purpose (vetting) and is necessary to fulfill the objectives of the system.
- Users are assigned roles based upon their responsibilities and a need-to-know basis. Each user and role is individually authorized.
- User accounts are authenticated via active directory
- The INVEST SharePoint home page and the application are not accessible publicly via the Internet

5. Retention

a. How long is information retained?

Information will be deleted or destroyed in accordance with vetting industry standards, where the default is to maintain a record for three years. Though it is not always realistic to follow, the Department records disposition schedule **A-30-009-01a-e** dictates that files are Destroy/delete ONLY after the final decision to accept, reject or suspend training or funding is made and forwarded to posts and the email has been captured as a "record email" in SMART and tagged with Subject TAGS PHUM.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Risk impact is minimal, as the retention schedule is sufficient for the type of information collected.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The information is shared with regional and functional bureaus on a need-to-know basis for the purpose of approving or denying foreign assistance and training from foreign security force candidates.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

The INVEST application notifies users with a need-to-know when files on a relevant applicant have been updated and are ready to be passed to them for processing. INVEST is a work-flow application, so it passes information from one user to the next (i.e. vetter to approver). The specific information is only accessible to authorized users via BPM software that manages the workflow between departments. Users comply with Department regulations for handling SBU material. The Operator's manual and training material warn about proper use of the information.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Information in INVEST is only shared with internal organizations on a need-to-know basis. The minimum amount of information is collected and shared, and controls like limited access and training mitigate the privacy risk from internal sharing.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

The INVEST system information is only shared with U.S. government employees with a need-to-know. The most common non-State sponsoring offices are FBI-LEGAT and

DEA. Additionally, a few military commands track INVEST when vetting is complete to enable them to plan the travel of their trainers.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

The INVEST system information is only shared with U.S. government employees with a need-to-know. The operator's manual and training material warn about proper use of the information.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The INVEST system information is only shared with US government employees with a need-to-know. The operator's manual and training material warn about proper use of the information.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

State-79, INVEST will cover this system.

does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Host foreign governments are informed that their units and individuals proposed for training are vetted for human rights violations. The U.S. Government does not notify the individual being vetted. Additionally, once the SORN is published, it will provide notice to individuals of the type of collection in INVEST.

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes. However, if the host foreign government or applicant fails to provide the information, they will not be approved for training or assistance.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. All information requested is necessary and is provided by the foreign government.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

If a unit or individual is not approved for training or assistance, the host foreign government is notified. Notices are not provided to the individual, due to the nature of the inquiries in INVEST. Additionally, notice is provided to individuals about the type of collection in INVEST through the forthcoming SORN mentioned earlier in this section.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Due to the nature of the inquiries in INVEST, individuals are not allowed to gain access to their information. If they were allowed to do so, the purpose of the system (i.e. vetting potential foreign security force candidates) would be compromised.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Notification and redress is handled by the foreign government due to the nature of the inquiries in INVEST. As a result, the lack of notification and redress mechanisms directly stemming from this system is justified by its purpose.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Access to INVEST is restricted to authorized users within the Department of State, domestic and post. All users receive training on properly operating INVEST and must maintain a security clearance. To utilize INVEST a user must be authorized to access the Department's unclassified computer network. Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited. Additionally, a user account is created in INVEST with group/user policies assigned.

b. What privacy orientation or training for the system is provided authorized users?

All users of the Department's computer network must complete annual computer security training and privacy information refresher training. Users will need to complete the annual training/refresher to remain active within INVEST.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Risks are similar to those stated in the computer security refresher program: shoulder surfing, not properly securing documents and computers, and failing to control passwords. However, these risks are properly mitigated by the safeguards discussed above, including restriction to authorized users, user access agreements, warning banners, monitoring and auditing, and security training.

11. Technologies

a. What technologies are used in the system that involves privacy risk?

There are no technologies being used that would elevate the risk factor.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

There are no technologies being used that would cause added privacy risk.

12. Security

What is the security certification and accreditation (C&A) status of the system?

Authorization to Operate granted on 4/15/2010. The next C&A certification is scheduled for 1st quarter, 2013 and is expected to be granted.